

Tencent Cloud CodeBuddy Security and Privacy Guide Product Documentation



Copyright Notice

©2013–2026 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

 Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by the Tencent corporate group, including its parent, subsidiaries and affiliated companies, as the case may be. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Security and Privacy Guide

Last updated: 2026-03-02 15:47:14

Sensitive Data Protection Recommendations

1. **Use environment variables** – Avoid hardcoding sensitive information in code
2. **Configuration file encryption** – Use tools like git-crypt to encrypt sensitive configuration
3. **Rotate credentials regularly** – Use `apiKeyHelper` to get key dynamically

Report a Security Issue

If a security vulnerability is detected, follow the process below:

1. **Do not disclose publicly** – Avoid discussing vulnerability details in public channels
2. **Contact us through official channels** – Security report channel is provided by
3. **Provide detailed information** – Include complete reproduction procedure and impact range
4. **Coordinated disclosure** – Provide a reasonable time window before issue fixing

Important Notice

Note:

Although these protection measures significantly reduce risk, no system has complete immunity to ALL attacks. Always maintain good security practice when using any AI tool.

User Responsibility: CodeBuddy IDE only has the permission granted by the user. The user is responsible for reviewing the security of suggested